12 FAM 500
INFORMATION SECURITY

12 FAM 510
CLASSIFICATION MANAGEMENT

(TL:DS-61; 10-01-1999)

12 FAM 511 POLICY AND PURPOSE

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

These regulations implement Executive Order (E.O.) 12356, National Security Information, April 2, 1982, which prescribes a uniform system for classifying, declassifying, and safeguarding national security information ("classified information").

12 FAM 511.1 Scope

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. These regulations apply to all information, both national security and otherwise, that is owned by, originated by, produced by or for, or under the control of Foreign Affairs Agencies, at any and all locations regardless of physical form. For purposes of these regulations, Foreign Affairs Agencies include the following:

   (1) The Department of State;

   (2) The Agency for International Development (A.I.D.);

   (3) The Overseas Private Investment Corporation (OPIC);

   (4) The Trade and Development Program (TDP); and

   (5) All other executive branch agency personnel located overseas under the jurisdiction of a chief of mission.

b. The Bureau of Diplomatic Security's Application Branch of the Information Security Programs Division of the Office of Information Security Technology (DS/ISP/APB) administers the Department of State's Information Security Program ("Program").

c. The Information Security Program within A.I.D. is established within the Inspector General's Office of Security (IG/SEC).

12 FAM 511.2 Applicability

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Unless otherwise noted herein, these regulations apply to all personnel of the Foreign Affairs Agencies.

b. Nothing in these regulations supersedes any requirement related to "Restricted Data" in the Atomic Energy Act of August 30, 1954, as amended, or Department of Energy regulations.

c. Sensitive compartmented information (SCI), special access programs (SAPs), and communications security (COMSEC) information shall be processed and controlled in accordance with applicable national authorities, directives, and policies.

d. These regulations also apply to information handled, stored, reproduced, or manipulated by automated information systems (AISs), also known as automated data systems.

e. For the Department of State, AIS security requirements are promulgated by DS/CIS/IST.

12 FAM 511.3 Authorities

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Except as provided for in the Atomic Energy Act of 1954, as amended, E.O. 12356, as implemented by ISOO Implementing Directives, and these regulations provide the only basis for classifying information.

b. See 12 FAM 511 regarding E.O. 12356. It also establishes a monitoring system to enhance its effectiveness.

c. Information Security Oversight Office (ISOO) Implementing Directive No. 1 sets forth guidance to agencies on original and derivative classification,

downgrading, declassification, and safeguarding of national security information.

d. The Omnibus Diplomatic Security and Antiterrorism Act of 1986, Pub. L. No. 99-399, codified at 22 U.S.C. 4804.

e. The legal authority for A.I.D. implementation of these regulations includes the Inspector General Act of 1978 (Pub. L. 95-452) as amended.

12 FAM 512 IMPLEMENTATION AND OVERSIGHT RESPONSIBILITIES

12 FAM 512.1 Responsibilities

12 FAM 512.1-1 The National Security Council (NSC)

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

The NSC provides overall policy direction for the Federal Government's Information Security Program pursuant to provisions of E.O. 12356.

12 FAM 512.1-2 Information Security Oversight Office (ISOO)

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. ISOO operates under the administrative auspices of the General Services Administration (GSA), while receiving its policy guidance from the National Security Council (NSC). The GSA Administrator, with the approval of the President, appoints the Director of the ISOO.

b. The Director, ISOO, is charged with the principal functions outlined in section 5.2(b) of E.O. 12356.

c. The Director, ISOO, may request information or material concerning the Program to carry out its functions.

d. The Bureau of Diplomatic Security is responsible for coordinating the Department's response to ISOO requirements.

e. Within A.I.D., the Office of the Inspector General is charged with coordinating responses to ISOO requirements.

12 FAM 512.1-3 Senior Agency Officials

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Individuals occupying the following positions are designated as senior agency officials:

(1) Department of State: Assistant Secretary for Diplomatic Security (DS);

(2) Agency for International Development (A.I.D.): Inspector General;

(3) The Overseas Private Investment Corporation (OPIC): Vice President for Management Services; *and*

(4) Trade and Development Program (TDP): Assistant Director for Management.

b. Senior agency officials have the primary responsibility to oversee their respective agency's Information Security Program. This includes the requirement to:

(1) Establish and monitor agency policies and procedures to ensure proper classification of material;

(2) Ensure the protection from unauthorized disclosure of classified information, including intelligence information;

(3) Ensure that a program of orderly and effective declassification of documents that no longer require protection in accordance with E.O. 12356 exists;

(4) Review proposed classified disclosures of an exceptional nature bearing upon issues of concern to the Congress and the public;

(5) Issue any needed guidelines for classification or declassification;

(6) Recommend to the agency head the following:

(a) Proposals to reclassify information previously declassified and disclosed if it is determined in writing that the information requires protection in the interest of national security, and the information may reasonably be recovered. This reclassification action must be reported promptly to the Director, ISOO;

(b) Determinations of other categories of information that are

related to the national security, other than those listed in E.O. 12356, which require protection against unauthorized disclosure. Report such determinations promptly to the Director, ISOO;

(7) Establish a security awareness program to educate employees concerning their duties and responsibilities with regard to the requirements of E.O. 12356;

(8) Prepare a list of officials, by position, delegated Top Secret, Secret, and Confidential original classification authority;

(9) Receive and take appropriate action on suggestions and complaints with respect to the agency's administration of the Program;

(10) Provide guidance concerning corrective or disciplinary action in unusually important cases involving unauthorized disclosure or refusal to declassify; and

(11) Maintain liaison with the Director, ISOO, and report as required by E.O. 12356.

12 FAM 512.1-4 Supervisors

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

The ultimate responsibility for safeguarding classified information rests with each supervisor to the same degree that the supervisor is charged with functional responsibility for the organizational unit. While certain employees may be assigned specific security responsibilities, such as Top Secret control officer or unit security officer, it is nevertheless the basic responsibility of supervisors to ensure that classified material entrusted to their organizational unit is handled in accordance with the procedures required by these regulations. Each supervisor should ensure that no single employee is assigned unreasonable security responsibilities in addition to usual administrative or functional duties.

12 FAM 512.1-5 Employees

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Each employee having access to and/or possession of classified material is responsible for the maintenance of the security of such material. For the purposes of these regulations, the term "employee" includes anyone who is

certified and/or authorized access to classified information by virtue of a contract, consulting agreement, detail, grant, appointment to an advisory panel, or otherwise.

12 FAM 512.1-6 Top Secret Control Officers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Personnel appointed as Top Secret control officers (TSCOs) have the responsibility to ensure that Top Secret material is properly safeguarded, to include origination, marking, accountability, storage, duplication, transmission, and destruction.

12 FAM 512.1-7 Regional, Post, or Unit Security Officers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Personnel assigned to these positions have the supervisory and/or the oversight responsibility to ensure that classified material entrusted to their organizational unit is handled in accordance with the procedures prescribed in these regulations.

12 FAM 512.2 Evaluations, Surveys, and Inspections

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The executive director of each bureau, and each regional security officer (RSO), shall maintain the Program designed to ensure compliance with the provisions of these regulations. The executive director is responsible for ensuring that the bureau has a designated security officer and shall work with that officer to ensure that all employees are aware of security requirements. Within A.I.D., IG/SEC is responsible for evaluating the effectiveness of the A.I.D. Information Security Program and ensuring that all regulatory requirements are met.

b. If there is a 24-hour cleared U.S. citizen presence in the chancery/consulate, any annex within that diplomatic compound could be considered an extension of the controlled access area, when the following contingencies are met:

(1) The annex offices storing classified materials are:

(a) During office hours, under pushbutton, cypher lock; and

(b) After hours, under DS-controlled key lock.

(2) The cleared U.S. citizen guards conduct periodic, random checks of this area.

(3) At high and critical threat posts, this area must also be alarmed.

This interpretation does not apply to offices or facilities outside the physical confines of the compound.

12 FAM 513 CLASSIFICATION DESIGNATIONS

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified with one of three designations: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only" and "Limited Official Use" shall not be used to identify classified information. (See subchapter 12 FAM 540.) Moreover, no other term such as "Sensitive," "Conference," or "Agency" shall be used in conjunction with the authorized classification designations to identify classified information.

12 FAM 513.1 Top Secret

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Information may be classified "Top Secret" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

b. Examples of "exceptionally grave damage" include:

(1) Armed hostilities against the United States or its allies;

(2) Disruption of foreign relations vitally affecting the national security;

(3) The compromise of vital national defense plans or complex cryptologic and communications intelligence systems;

(4) The revelation of sensitive intelligence operations; and

(5) The disclosure of scientific or technological developments vital to national security.

12 FAM 513.2 Secret

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Information may be classified "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

b. Examples of "serious damage" include:

(1) Disruption of foreign relations significantly affecting the national security;

(2) Significant impairment of program or policy directly related to the national security;

(3) Revelation of significant military plans or intelligence operations; and

(4) Compromise of significant scientific or technological developments relating to national security.

12 FAM 513.3 Confidential

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

b. An example of "damage" includes release of information that might cause a foreign government to hesitate in confiding in the United States.

12 FAM 514 AUTHORITY TO CLASSIFY, DOWNGRADE AND DECLASSIFY

12 FAM 514.1 Original Classification Authority

12 FAM 514.1-1 Top Secret

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

In the Department of State, authority to classify information originally as Top Secret may be exercised by the Secretary; the Assistant Secretary for Diplomatic Security, as the senior agency official; and officials to whom the Secretary or the senior official delegate this authority on the basis of their frequent need to exercise such authority. Normally these will not be below the level of deputy assistant secretary in the Department; or chief of mission, chargé d'affaires, or principal officer at an autonomous consular post overseas.

12 FAM 514.1-2 Secret

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Authority for original classification of information as "Secret" may be exercised by officials with Top Secret authority *such as the* the Administrator of A.I.D., or his or her senior official. This authority may also be delegated to subordinate officials by the Secretary or the senior agency official in the Department of State, the Administrator of A.I.D., or his or her senior official or an official with original Top Secret classification authority, who may designate in writing, by name or by position, on the basis of a frequent need to exercise such authority. Normally the individual receiving the delegated authority will not be below the level of office director, section head (in a mission abroad), country public affairs officer, or the equivalent.

12 FAM 514.1-3 Confidential

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Authority for original classification of information as "Confidential" may be exercised by officials with Top Secret or Secret classification authority, and the President of the Overseas Private Investment Corporation. This authority may be delegated to subordinate officials by the Secretary or the senior official in the Department of State, the Administrator of A.I.D., or an official with original Top Secret classification authority, who may designate in writing, by name or by position, on the basis of a frequent need to exercise such authority.

12 FAM 514.1-4 Redelegation Prohibited

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Delegated original classification authority at any level may not be redelegated.

12 FAM 514.1-5 Absence of Authorized Classifier

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

In the absence of an authorized classifier, the person designated to act for that official may exercise the classifying authority.

12 FAM 514.1-6 Listing Authorized Classifiers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. In the Department of State, DS/ISP/APB; in A.I.D., the Office of Security; and in OPIC, the Vice President for Management Services, shall maintain a current listing, by classification designation, of the positions of officials carrying original classification authority.

b. The listing shall be reviewed as needed to ensure that such delegations have been held to a minimum, and that officials so designated have a continuing need to exercise such authority, and that newly appointed original classification authorities are properly and promptly briefed on their duties and responsibilities.

12 FAM 514.1-7 Requests for Classification Authority Pursuant to E.O. 12356

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. A request for original classification authority shall be made only when there is a demonstrable and continuing need to exercise such authority and the following conditions exist:

(1) The normal course of operations or missions of the organization results in the origination of information warranting classification;

(2) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of

authority or supervision for relatively detailed guidance;

(3) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek knowledge from a higher level of authority of supervision; and

(4) There is a valid reason why already designated classification authorities in the originator's chain of authority or supervision have not issued or cannot issue classification guidance to meet the originator's normal needs.

b. See 12 FAM 518.1 for processing request for delegation of original classification authority.

12 FAM 514.1-9 Training Requirements for Original Classification Authorities

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Senior agency officials, chiefs of mission, and heads of bureaus and operating components domestically, shall ensure that all original classification authorities are fully versed in the fundamentals of security classification, limitations of their authority, and responsibilities.

12 FAM 514.2 Derivative Classification Authority

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Derivative classification is made by a person, not necessarily having original classification authority, based on an originally classified document or as directed by a classification guide. The derivative classifier may reproduce, extract, restate, paraphrase, or summarize classified materials, or apply markings in accordance with source material or a classification guide.

b. Derivative classifiers must respect original classification markings. Only if the derived document, by means of paraphrasing, excising, etc., has clearly lost the original grounds for classification may its original classification be removed or lowered.

c. Subject to 12 FAM 514.2, paragraph b, markings on derivatively classified material, including declassification instructions, shall be carried forward from the original material or shall be directed by the classification guide.

Verify the information's current level of classification as far as practicable before applying the markings.

12 FAM 515 REQUIREMENTS

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. To be eligible for classification, material must meet the requirements of section 1.3 of E.O. 12356.

b. The material must be U.S. Government owned or controlled.

c. An official with original classification authority must determine that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

d. Certain information that would otherwise be unclassified may require classification when combined or associated with other classified (i.e., classification by association) or unclassified information (i.e., classification by compilation). Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or record copy of the information.

12 FAM 516 STANDARDS

12 FAM 516.1 Classification

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Information shall remain classified for as long as required by national security considerations. E.O. 12356 requires that each decision to classify dictates a simultaneous determination of the duration such classification must remain in force or that the duration of classification cannot be determined.

b. If there is reasonable doubt about the need to classify information, safeguard the information as if it were Confidential pending a

determination by an original classification authority about its classification. If there is reasonable doubt about the appropriate classification level, safeguard the information at the higher level pending the determination by an original classification authority of its classification level. Determinations under this section shall be made within 30 calendar days. Upon final determination of classification, all information shall be properly marked.

c. Do not classify information unless its disclosure reasonably could be expected to cause damage to the national security. Information may not be classified to:

   (1) Conceal violations of law, inefficiency, or administrative error;

   (2) Prevent embarrassment to a person, organization, or agency;

   (3) Restrain competition; or

   (4) Prevent or delay the release of information that does not require protection in the interest of national security.

d. Each document and portion thereof shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference standing alone reveals classified information. The overall classification of a document or group of physically connected documents shall be at least as high as that of the most highly classified component. The subject or title of a classified document normally should be unclassified.

12 FAM 516.2 Declassification

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Declassify or downgrade information as soon as national security considerations permit. Decisions concerning declassification shall be based on the loss of information sensitivity with the passage of time or upon the occurrence of a specific event. Information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure of identical or similar information. However, such disclosures require immediate determination of the degree of damage to the national security and re-evaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted.

12 FAM 516.3 Reclassification

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The President or an agency head or official designated under sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) of E.O. 12356 may reclassify information previously declassified and disclosed if it is determined in writing that:

(1) The information requires protection in the interest of national security; and

(2) The information may reasonably be recovered.

Report these reclassification actions promptly to the Director, ISOO.

b. Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552, as amended, hereinafter referred to as FOIA) or the Privacy Act (5 U.S.C. 552a) or the mandatory review provisions of E.O. 12356, provided that such classification meets the requirements of E.O. 12356 and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official, or an official with original Top Secret classification authority. Classifiers should make every effort to classify properly at the time of origin. When a determination is made that a document requires classification or reclassification, however, the office making that determination should notify all holders of the document; and, in the Department of State, should send a copy of the classification or reclassification memorandum to the Office of Freedom of Information, Privacy, and Classification Review (A/IM/IS/FPC). Within A.I.D., send copies to XA/PI.

12 FAM 516.4 Reclassification Authorities

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. For the Department of State, the Assistant Secretary for Diplomatic Security performs these functions.

b. For A.I.D. and OPIC, the Administrator, and the Vice President for Management Services, respectively, perform the function.

12 FAM 517 CLASSIFICATION RESPONSIBILITIES

12 FAM 517.1 Accountability of Classifiers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Classifiers are accountable for the propriety of the classifications they assign, whether by exercise of original classification authority or by derivative classification.

b. An official who classifies a document or other material continues to be accountable even though the document or material is approved or signed at a higher level in the same organization.

c. When an official signs or approves a document or other material already marked to reflect a particular level of classification, that official shall review the information contained therein to determine if the classification markings are appropriate.

d. A higher level official through or to whom a document or other material passes for signature or approval becomes jointly responsible with the accountable classifier for the classification assigned. Such official has discretion to decide whether a subordinate who has classification authority shall be identified as the accountable classifier when he or she has exercised that authority.

e. Advance classification planning is an essential part of the drafting of any document or in the development of any plan, program, or procurement action that involves classified information. The responsible official should consider classification from the outset to ensure adequate protection for the information and to eliminate impediments to the delivery, execution, or implementation of the document, plan, program, project, or procurement action. The official charged with the drafting or developing of any plan, program or project in which classification is a factor shall include, under an identifiable title or heading, classification guidance covering the information involved. The guidance shall conform to the requirements contained in E.O. 12356. Classifiers should strive to use unclassified subjects or titles to allow their use in totally unclassified documents, or without creating another classified document.

f. Within A.I.D., classification guides are required for classified programs of a recurring or continuous nature. The sponsor of the program or project is responsible for the development of a guide containing the following

elements:

(1) The groups or categories of information to be protected;

(2) The applicable classification level for each group or category of information;

(3) Declassification instructions for each group or category of information in terms of time, an event, or the notation OADR; and

(4) Approval and signature of an official with responsibility for the information and who is authorized to classify information originally at the highest level of classification prescribed by the guide.

g. Program/project sponsors must send a copy of all classification guides generated within A.I.D. to IG/SEC. Sponsors must review classification guides at least every two years and update them as necessary.

12 FAM 517.2 Challenges to Classification

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

If holders or recipients of classified information have substantial reason to believe that the information is improperly classified or, in fact, unclassified, they shall communicate that belief to the classifier of the information or other responsible officials to bring about any necessary correction. See 12 FAM 518.2 for guidelines on challenging classification.

12 FAM 518 PROCEDURES FOR CLASSIFICATION MANAGEMENT

12 FAM 518.1 Requests for Classification Authority Pursuant to E.O. 12356

(TL:DS-40; 10-12-1994)

Each request for a delegation of original classification authority shall:

(1) Identify the title of the position held by the nominee and the nominee’s organization;

(2) Contain a description of the circumstances, consistent with 12 FAM 514.1-7, that justify the delegation of such authority;

(3) Be submitted in the Department of State through DS/CIS/IST through the Deputy Assistant Secretary for DS/CIS to the Assistant Secretary for Diplomatic Security or to the Secretary; and

(4) Be submitted within A.I.D. through the Inspector General to the Administrator, A.I.D.

12 FAM 518.2 Challenging Classification

(TL:DS-40; 10-12-1994)

a. Challenges to classification made under this section shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification shall also include the reason(s) why the challenger believes that the information is classified improperly or unnecessarily.

b. Classifying officers receiving challenges pursuant to this section shall act upon them within 30 calendar days of receipt. The classifying officer shall notify the challenger of any changes made as a result of the challenge or the reasons why no change is made.

c. Pending final determination of a challenge to classification, safeguard the information or document in question as required for the level of classification initially assigned.

d. The fact that an employee of the Department of State has issued a challenge to classification shall not in any way result in or serve as a basis for adverse personnel action.

e. The provisions of this section do not apply to or affect declassification review actions undertaken under the mandatory review requirements of 5 FAM or under provisions of the FOIA.

f. If not resolved at a lower level, refer challenges to classification involving more than one bureau or post to DS, through DS/CIS/IST, for resolution. Challenges to classification involving the Department of State and another Agency or Department of the U.S. Government that are not resolved may be referred to the Director, ISOO, by the Bureau of Diplomatic Security.

g. Within A.I.D., challenges to classification should be made to the cognizant classifier of the information. If unresolved, the challenger may appeal the decision through the Inspector General to the Administrator. If resolution cannot be obtained within A.I.D., further appeal may be made to ISOO.

12 FAM 519 UNASSIGNED